TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 334, Number 2, December 1992

ON THE GENERALIZED RAMANUJAN-NAGELL EQUATION $x^2 - D = 2^{n+2}$

LE MAOHUA

ABSTRACT. Let D be a positive integer which is odd. In this paper we prove that the equation $x^2 - D = 2^{n+2}$ has at most three positive integer solutions (x, n) except when $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$, where m is a positive integer with $m \geq 3$.

1. INTRODUCTION

Let $\mathbf{Z}$, $\mathbf{N}$, $\mathbf{Q}$ be the sets of integers, positive integers and rational numbers respectively. Let $D \in \mathbf{N}$ be odd, and let $N(D)$ denote the number of solutions (x, n) of the generalized Ramanujan-Nagell equation

(1) $$\chi^2 - D = 2^{n+2}, \qquad \chi > 0, n > 0.$$ [1]

In [1], Beukers proved that $N(D) \leq 4$. Simultaneously, he showed that if $N(D) > 3$, then D must be among the following types:

(I) $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$, $m \in \mathbf{N}$, $m \geq 3$.

(II) $D = ((2^{2m+1} - 17)/3)^2 - 32$, $m \in \mathbf{N}$, $m \geq 3$.

(III) $D = 2^{2m_2} + 2^{2m_1} - 2^{m_2+m_1+1} - 2^{m_2+1} - 2^{m_1+1} + 1$, [2] $m_1, m_2 \in \mathbf{N}$, $m_2 > m_1 + 1 > 2$.

Moreover, equation (1) has exactly four solutions $(x, n) = (2^m - 3, 1)$, $(2^m - 1, m)$, $(2^m + 1, m + 1)$, and $(3 \cdot 2^m - 1, 2m + 1)$ if D is of type I. In this paper, we completely determine all D for which $N(D) = 4$.

Theorem. *If D is of type* I, *then* $N(D) = 4$ *otherwise* $N(D) \leq 3$.

2. PRELIMINARIES

Lemma 1 [3, Formula 1.76]. *For any $m \in \mathbf{N}$ and any complex numbers α, β, we have*

$$\alpha^m + \beta^m = \sum_{i=0}^{[m/2]} (-1)^i \begin{bmatrix} m \\ i \end{bmatrix} (\alpha + \beta)^{m-2i} (\alpha\beta)^i,$$

Received by the editors March 30, 1990 and, in revised form, September 18, 1990.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 11D61.

[1] Throughout this paper, "solution" and "positive solution" are the abbreviations for "integer solution" and "positive integer solution" respectively.

[2] In [1] there is a misprint in this expression.

where

$$\begin{bmatrix} m \\ i \end{bmatrix} = \frac{(m-i-1)!m}{(m-2i)!i!}, \qquad i = 0, \dots, \left[\frac{m}{2}\right],$$

are positive integers. □

Lemma 2 [2, Theorem 6.10.3]. *Let a/b, a'/b', $a''/b'' \in \mathbf{Q}$ be positive with $ab' - a'b = \pm 1$. If a''/b'' lies in the interval $(a/b, a'/b')$, then there exist positive integers c, c' such that*

$$a'' = ca + c'a', \qquad b'' = cb + c'b'. \quad \square$$

Lemma 3. *If (U, V) is a positive solution of the equation*

$$U^2 - 2V^2 = 1 \tag{2}$$

with $2^{m+1}|V$ for some $m \in \mathbf{N}$, then $U + V\sqrt{2} = (3+2\sqrt{2})^{2^m t}$ for some $t \in \mathbf{N}$.

Proof. Since $3 + 2\sqrt{2}$ is the fundamental solution of equation (2), we have $U + V\sqrt{2} = (3+2\sqrt{2})^{\gamma}$ for some $\gamma \in \mathbf{N}$. Then

$$V = \sum_{i=0}^{((r-1)/2)} \binom{\gamma}{2i+1} 3^{\gamma-2i-1} 2^{3i+1}. \tag{3}$$

If $2^{m+1}|V$, then from (3) we see that $2|\gamma$. Further, if $2^{\lambda}\|\gamma$, since

$$\binom{\gamma}{2j+1} 2^{3j+1} = \gamma \binom{\gamma-1}{2j} \frac{2^{3j+1}}{2j+1} \equiv 0 \pmod{2^{\lambda+2}} \quad \text{for } j > 0,$$

we obtain $\lambda \geq m$ by (3). The lemma is proved. □

Let $d \in \mathbf{N}$ be nonsquare, and let $k \in \mathbf{Z}$ with $\gcd(k, d) = 1$.

Lemma 4 [2, Theorem 10.8.2]. *If $|k| < \sqrt{d}$ and (X, Y) is a positive solution of the equation*

$$X^2 - dY^2 = k, \qquad \gcd(X, Y) = 1, \tag{4}$$

then X/Y is a convergent of $\sqrt{d}$. □

It is a well-known fact that the simple continued fraction of $\sqrt{d}$ can be expressed as $[a_0, a_1, \dots, a_s]$, where $a_0 = (\sqrt{d})$, $a_s = 2a_0$, and $a_i < 2a_0$ for $i = 0, \dots, s-1$.

Lemma 5. *For any nonnegative integer j, let p_j/q_j and γ_j denote the jth convergent and complete quotient of $\sqrt{d}$ respectively. Further let*

$$k_j = (-1)^{j-1}(p_j^2 - dq_j^2) \quad \text{and} \quad \Delta_j = (-1)^j(p_{j-1}p_j - dq_{j-1}q_j).$$

Then we have:

(i) $k_j > 0$, $\Delta_j > 0$, *and*

$$a_{j+1} = \left[\frac{\Delta_j + \sqrt{d}}{k_j}\right]. \tag{5}$$

(ii) $k_j = 1$ *if and only if* $a_{j+1} = 2a_0$.

(iii) *Let*

$$t = \begin{cases} s-1, & \text{if } 2|s, \\ 2s-1, & \text{if } 2 \nmid s. \end{cases}$$

Then $p_t + q_t\sqrt{d}$ *is the fundamental solution of the equation*

$$u^2 - dv^2 = 1. \tag{6}$$

(iv) *For any* $m \in \mathbf{N}$, $k_{ms+i} = k_i \quad (i = 0, \dots, s-1)$.

(v) *If* $1 < k < \sqrt{d}$, $2d \not\equiv 0 \pmod{k}$ *and equation* (4) *has solutions* (X, Y), *then it has at least two positive solutions such that*

$$X < p_t, \qquad Y < q_t. \tag{7}$$

Proof. Since $\frac{p_0}{q_0} < \cdots < \frac{p_{2m}}{q_{2m}} < \frac{p_{2m+2}}{q_{2m+2}} < \cdots < \sqrt{d} < \cdots < \frac{p_{2m+1}}{q_{2m+1}} < \frac{p_{2m-1}}{q_{2m-1}} < \cdots < \frac{p_1}{q_1}$ for any $m \in \mathbf{N}$, we get $k_j > 0$ and $\Delta_j > 0$. Since $p_{j-1}q_j - p_jq_{j-1} = (-1)^j$, we have

$$p_j = \Delta_j q_j + k_j q_{j-1}, \qquad dq_j = \Delta_j p_j + k_j p_{j-1}, \tag{8}$$

$$d = \Delta_j^2 + k_{j-1}k_j. \tag{9}$$

So we obtain

$$\gamma_{j+1} = -\frac{p_{j-1} - q_{j-1}\sqrt{d}}{p_j - q_j\sqrt{d}} = -\frac{(p_{j-1} - q_{j-1}\sqrt{d})(p_j + q_j\sqrt{d})}{(p_j - q_j\sqrt{d})(p_j + q_j\sqrt{d})} = \frac{\Delta_j + \sqrt{d}}{k_j}. \tag{10}$$

Since $a_{j+1} = [\gamma_{j+1}]$, (5) is proved by (10).

If $k_j = 1$, then from (8) we get

$$p_j/q_j = \Delta_j + q_{j-1}/q_j. \tag{11}$$

From

$$\left[\frac{q_{j-1}}{q_j}\right] = \begin{cases} 1, & \text{if } j = 1 \text{ and } q_0 = q_1 = 1, \\ 0, & \text{otherwise}, \end{cases}$$

we obtain $\Delta_j = a_0$ by (11), and $a_{j+1} = 2a_0$ by (5). On the other hand, if $a_{j+1} = 2a_0$, since $\Delta_j < \sqrt{d}$ by (9), then we have $k_j = 1$ by (5). Thus (ii) is proved.

By (ii), (iii) is clear. In addition, (iv) is Theorem 10.8.3 of [2].

Let (X, Y) be a solution of equation (4). Since $k > 1$ implies $XY \neq 0$, then $(|X|, |Y|)$ is a positive solution of equation (4). By Lemma 4, $|X|/|Y|$ is a convergent of $\sqrt{d}$ since $k < \sqrt{d}$. Hence $|X|/|Y| = p_{2r+1}/q_{2r+1} \quad (\gamma \geq 0)$. Then there exists the integers a, i such that $a \geq 0$, $2|as$, $2 \nmid i$, and $0 < i < t$, since $k > 1$. By (iv), we have $k_i = k$. It follows that (p_i, q_i) is a positive solution of equation (4) with (7). Let

$$X' = p_i p_t - dq_i q_t, \qquad Y' = p_i q_t - p_t q_i. \tag{12}$$

Then X', Y' are coprime integers. From

$$X'^2 - dY'^2 = (p_i^2 - dq_i^2)(p_t^2 - dq_t^2) = k,$$

we see that (X', Y') is a solution of equation (4). Further, (X', Y') is a positive solution by

$$0 < X' - Y'\sqrt{d} = (p_i + q_i\sqrt{d})(p_t - q_t\sqrt{d}) = \frac{p_i + q_i\sqrt{d}}{p_t + q_t\sqrt{d}} < 1.$$

By Lemma 4, X'/Y' is a convergent of $\sqrt{d}$. From

$$X' + Y'\sqrt{d} = (p_i - q_i\sqrt{d})(p_t + q_t\sqrt{d}) < p_t + q_t\sqrt{d},$$

we get $X' < p_t$ and $Y' < q_t$. If $(X', Y') = (p_i, q_i)$, since $\gcd(p_i, q_i) = 1$, then from (12) we get

$$p_t - 1 = c_1 q_i, \quad dq_t = c_1 p_i, \quad p_t + 1 = c_2 p_i, \quad q_t = c_2 q_i, \qquad c_1, c_2 \in \mathbf{N}.$$

Since $c_1 p_i = c_2 d q_i$, we have $c_1 = c q_i$, $c_2 d = c p_i$, where $c \in \mathbf{N}$. Hence $2d = c_2 d p_i - c_1 d q_i = c(p_i^2 - d q_i^2) = ck \equiv 0 \pmod{k}$, a contradiction. Therefore $(X', Y') \neq (p_i, q_i)$, (v) is proved. □

Let $I(d) = \{(d_1, d_2) | d_1, d_2 \in \mathbf{N},\ d_1 d_2 = d,\ \gcd(d_1, d_2) = 1\}$, and let $I'(d) = I(d) \backslash \{(1, d)\}$.

Lemma 6 [4]. *There exists at most one pair $(d_1, d_2) \in I'(d)$ which make the equation*

$$d_1 u'^2 - d_2 v'^2 = 1 \tag{13}$$

has solutions (u', v'). □

Lemma 7 [2, Theorems 11.4.1 and 11.4.2]. *Let $(d_1, d_2) \in I(d)$. If (X, Y) is a solution of the equation*

$$d_1 X^2 - d_2 Y^2 = k, \qquad \gcd(X, Y) = 1, \tag{14}$$

then there exists a unique integer l such that

$$l = d_1 \alpha X - d_2 \beta Y, \qquad 0 < l \leq |k|,$$

where $\alpha, \beta \in \mathbf{Z}$ with $\beta X - \alpha Y = 1$. Such l is called the characteristic number of the solution (X, Y), and it will be denoted by $\langle X, Y \rangle$. If $\langle X, Y \rangle = l$, then we have

$$d_1 X \equiv -lY \pmod{k}, \quad l^2 \equiv d \pmod{k}, \quad \gcd\left(k, 2l, \frac{l^2 - d}{k}\right) = 1. \quad \square$$

Lemma 8 [2, Theorem 11.4.2]. *Let (X_1, Y_1), (X_2, Y_2) be solutions of equation (14). Then $\langle X_1, Y_1 \rangle = \langle X_2, Y_2 \rangle$ if and only if*

$$X_2 \sqrt{d_1} + Y_2 \sqrt{d_2} = (X_1 \sqrt{d_1} + Y_1 \sqrt{d_2})(u + v\sqrt{d}),$$

where (u, v) is a solution of equation (6). □

Lemma 9. *If $2 \nmid d$ and the congruence*

$$l^2 \equiv d \pmod{2^{m+2}}, \qquad 0 < l \leq 2^{m+2}, \qquad \gcd\left(2^{m+2}, 2l, \frac{l^2 - d}{2^{m+2}}\right) = 1, \tag{15}$$

has a solution l for $m \in \mathbf{N}$, then it has exactly one solution $l' = 2^{m+2} - l$ with $l' \neq l$.

Proof. Let l' be a solution of (15) with $l' \neq l$. Since $2 \nmid d$ implies $2 \nmid ll'$, we get from $l^2 \equiv l'^2 \equiv d \pmod{2^{m+2}}$ that $l' \equiv \delta l \pmod{2^{m+1}}$, where $\delta \in \{-1, 1\}$. If $\delta = 1$, then $l' = l + 2^{m+1} t$ for some $t \in \mathbf{Z}$. Notice that $2 \nmid (l^2 - d)/2^{m+2}$ and $2 \nmid (l'^2 - d)/2^{m+2}$. From

$$\frac{l'^2 - d}{2^{m+2}} = \frac{l^2 - d}{2^{m+2}} + lt + 2^m t^2,$$

we get $2 \mid t$, and so $l' = l$ since $0 < l,\ l' \le 2^{m+2}$. This is a contradiction. Hence $\delta = -1$. Then $l' = -l + 2^{m+1}t$ for some $t \in \mathbf{Z}$. From

$$\frac{l'^2 - d}{2^{m+2}} = \frac{l^2 - d}{2^{m+2}} - lt + 2^m t^2,$$

we obtain $l' = 2^{m+2} - l$ since $0 < l,\, l' \le 2^{m+2}$. The lemma is proved. □

Lemma 10. *Let* $m \in \mathbf{N}$, *and let* $(d_1, d_2) \in I(d)$. *If* $2 \nmid d$ *and* (X_0, Y_0) *is a solution of the equation*

$$d_1X^2 - d_2Y^2 = 2^{m+2}, \qquad \gcd(X, Y) = 1, \tag{16}$$

then all the solutions of equation (16) *are given by*

$$X\sqrt{d_1} + Y\sqrt{d_2} = (X_0\sqrt{d_1} + Y_0\sqrt{d_2})(u + v\sqrt{d}),$$

where (u, v) *is an arbitrary solution of equation* (6).

Proof. Under the assumption, $(X_0, -Y_0)$ is a solution of equation (16) too. Let $l = \langle X_0, Y_0\rangle$. Then $\langle X_0, -Y_0\rangle \equiv -l \pmod{2^{m+2}}$. By Lemma 9, we have either $\langle X, Y\rangle = \langle X_0, Y_0\rangle$ or $\langle X, Y\rangle = \langle X_0, -Y_0\rangle$ for any solution (X, Y) of equation (16). Thus, by Lemma 8, the lemma is proved. □

Lemma 11. *If* $2 \nmid d$ *and the equation*

$$X^2 - dY^2 = 2^{z+2}, \qquad \gcd(X, Y) = 1, \qquad Z > 0, \tag{17}$$

has solutions (X, Y, Z), *then it has a unique positive solution* (X_1, Y_1, Z_1) *such that*

$$Z_1 \le Z, \qquad 1 < \frac{X_1 + Y_1\sqrt{d}}{X_1 - Y_1\sqrt{d}} < (u_1 + v_1\sqrt{d})^2, \tag{18}$$

where Z *runs over all solutions of equation* (17), $u_1 + v_1\sqrt{d}$ *is the fundamental solution of equation* (6). *Such* (X_1, Y_1, Z_1) *is called the least solution of equation* (17). *Moreover, all solutions of equation* (17) *are given by*

$$Z = Z_1 t, \qquad \frac{X + Y\sqrt{d}}{2} = \left(\frac{X_1 \pm Y_1\sqrt{d}}{2}\right)^t (u + v\sqrt{d}),$$

where t *is an arbitrary positive integer,* (u, v) *is an arbitrary solution of equation* (6).

Proof. Let (X_0, Y_0, Z_1) be a solution of equation (17) with $Z_1 \le Z$. By Lemma 10, all solutions of equation (17) with $Z = Z_1$ are given by

$$X + Y\sqrt{d} = (X_0 \pm Y_0\sqrt{d})(u + v\sqrt{d}). \tag{19}$$

Since $u + v\sqrt{d} = \pm(u_1 + v_1\sqrt{d})^\gamma$ $(\gamma \in \mathbf{Z})$, we see from (19) that equation (17) has a unique positive solution (X_1, Y_1, Z_1) which satisfy (18).

For any $t \in \mathbf{N}$, let

$$\frac{X_t + Y_t\sqrt{d}}{2} = \left(\frac{X_1 + Y_1\sqrt{d}}{2}\right)^t,$$

and let

$$\varepsilon = \frac{X_1 + Y_1\sqrt{d}}{2}, \qquad \overline{\varepsilon} = \frac{X_1 - Y_1\sqrt{d}}{2}.$$

By Lemma 1, we have

$$X_t = \varepsilon^t + \overline{\varepsilon}^t = \sum_{i=0}^{[t/2]}(-1)^i \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon + \overline{\varepsilon})^{t-2i}(\varepsilon\overline{\varepsilon})^i = \sum_{i=0}^{[t/2]}(-1)^i \begin{bmatrix} t \\ i \end{bmatrix} X_1^{t-2i}2^{z_1 i},$$

$$Y_t = \frac{\varepsilon^t - \overline{\varepsilon}^t}{\sqrt{d}} = \begin{cases} \dfrac{\varepsilon - \overline{\varepsilon}}{\sqrt{d}} \displaystyle\sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon - \overline{\varepsilon})^{t-2i-1}(\varepsilon\overline{\varepsilon})^i \\ \qquad = Y_1 \displaystyle\sum_{i=0}^{(t-1)/2} \begin{bmatrix} t \\ i \end{bmatrix} (dY_1^2)^{(t-1)/2-i}2^{z_1 i}, \quad if\, 2 \nmid t, \\ \dfrac{\varepsilon^{t'} - \overline{\varepsilon}^{t'}}{\sqrt{d}} \displaystyle\prod_{j=0}^{(\alpha-1)} (\varepsilon^{2^j t'} + \overline{\varepsilon}^{2^j t'}) = \left(Y_1 \displaystyle\sum_{i=0}^{(t'-1)/2} \begin{bmatrix} t' \\ i \end{bmatrix} (dY_1^2)^{(t'-1)/2-i}2^{z_1 i}\right) \\ \qquad \times \displaystyle\prod_{j=0}^{\alpha-1} \left(\sum_{i=0}^{[2^j t'/2]} (-1)^i \binom{2^j t'}{i} X_1^{2^j t' - 2i} 2^{z_1 i} \right), \\ \qquad if\, t = 2^\alpha t',\, \alpha > 0,\, 2 \nmid t'. \end{cases}$$

Since $2 \nmid X_1Y_1$ implies $2 \nmid X_tY_t$, we see that $(X_t, Y_t, Z_1 t)$ is a solution of equation (17). Further, by Lemma 10, all solutions of equation (17) with $Z_1 | Z$ are given by

$$Z = Z_1 t, \qquad \frac{X + Y\sqrt{d}}{2} = \left(\frac{X_t \pm Y_t\sqrt{d}}{2}\right)(u + v\sqrt{d}) = \left(\frac{X_1 \pm Y_1\sqrt{d}}{2}\right)^t (u + v\sqrt{d}).$$

Let (X', Y', Z') be a solution of equation (17) with $Z_1 \nmid Z'$. Then $Z' = Z_1 t + Z_0$, where $t, Z_0 \in \mathbf{N}$ satisfy $Z_0 < Z_1$. Let $l = \langle X_t, Y_t \rangle$, and let $l' = \langle X', Y' \rangle$. By Lemma 7, we have

$$\begin{aligned} l^2 &\equiv d \pmod{2^{z_1 t+2}}, & l'^2 &\equiv d \pmod{2^{z'+2}}, \\ X_t &\equiv -lY_t \pmod{2^{z_1 t+2}}, & X' &\equiv -l'Y' \pmod{2^{z'+2}}. \end{aligned} \tag{20}$$

Since $2 \nmid ll'$, we get $l' \equiv \delta l \pmod{2^{z_1 t+2}}$, where $\delta \in \{-1, 1\}$. From (20),

$$X_tX' - \delta dY_tY' \equiv 0 \pmod{2^{z_1 t+2}}, \qquad X_tY' - \delta X'Y_t \equiv 0 \pmod{2^{z_1 t+2}}.$$

There exists the integers X'', Y'' such that

$$X_tX' - \delta dY_tY' = 2^{z_1 t+2}X'', \qquad X_tY' - \delta X'Y_t = 2^{z_1 t+2}Y''. \tag{21}$$

Then

$$X'Y'(X_t^2 - dY_t^2) \equiv 0 \pmod{\gcd(2^{z_1 t+2}X'', 2^{z_1 t+2}Y'')}.$$

Since $2 \nmid X'Y'$, we get $2 \nmid \gcd(X'', Y'')$. From (21) and

$$2^{z'+z_1 t+4} = (X_t^2 - dY_t^2)(X'^2 - dY'^2) = (X_tX' - \delta dY_tY')^2 - d(X_tY' - \delta X'Y_t)^2,$$

we have

$$X''^2 - dY''^2 = 2^{z_0}.$$

Since $d \equiv 1 \pmod 8$ implies $Z_0 > 2$, we see that $(X'', Y'', Z_0 - 2)$ is a solution of equation (17) with $Z < Z_1$, a contradiction. The lemma is proved. □

Lemma 12. *Let* $(d_1, d_2) \in I'(d)$. *If* $2 \nmid d$ *and the equation*

$$(22)\qquad d_1X'^2 - d_2Y'^2 = 2^{z'+2}, \qquad \gcd(X', Y') = 1, \qquad Z' > 0,$$

has solutions (X', Y', Z') *then equation* (17) *has solutions* (X, Y, Z). *Moreover, if equation* (13) *has solutions* (u', v'), *then all solutions of equation* (22) *are given by*

$$(23)\qquad Z' = Z, \qquad X'\sqrt{d_1} + Y'\sqrt{d_2} = (X + Y\sqrt{d})(u'\sqrt{d_1} + v'\sqrt{d_2}),$$

where (X, Y, Z) *and* (u', v') *are arbitrary solutions of equations* (17) *and* (13) *respectively. If equation* (13) *has no solution, then all solutions of equation* (22) *are given by*

$$(24)\qquad Z' = Z_1't', \qquad \frac{X'\sqrt{d_1} + Y'\sqrt{d_2}}{2} = \left(\frac{X_1'\sqrt{d_1} \pm Y_1'\sqrt{d_2}}{2}\right)^{t'}(u + v\sqrt{d})$$

where t' *is an arbitrary positive integer with* $2 \nmid t'$, (u, v) *is an arbitrary solution of equation* (6), (X_1', Y_1', Z_1') *is a unique positive solution of equation* (22) *such that*

$$(25)\qquad Z_1' = \frac{Z_1}{2}, \quad 1 < \frac{X_1'\sqrt{d_1} + Y_1'\sqrt{d_2}}{X_1'\sqrt{d_1} - Y_1'\sqrt{d_2}} < (u_1 + v_1\sqrt{d})^2,$$

where (X_1, Y_1, Z_1) *is the least solution of equation* (17), $u_1 + v_1\sqrt{d}$ *is the fundamental solution of equation* (6). *Such* (X_1', Y_1', Z_1') *is called the least solution of equation* (22).

Proof. Let (X', Y', Z') be a solution of equation (22). Then

$$\left(\frac{d_1X'^2 + d_2Y'^2}{2}\right)^2 - d(X'Y')^2 = 2^{2z'+2},$$

where $(d_1X'^2 + d_2Y'^2)/2$ and $X'Y'$ are coprime integers. It follows that equation (17) has solutions.

If equation (13) has solutions, then (23) gives out all solutions of equation (22) clearly.

If equation (13) has no solution, by Lemma 10, equation (22) has a unique positive solution (X_1', Y_1', Z_1') satisfies $Z_1' \le Z'$ and

$$1 < \frac{X_1'\sqrt{d_1} + Y_1'\sqrt{d_2}}{X_1'\sqrt{d_1} - Y_1'\sqrt{d_2}} < (u_1 + v_1\sqrt{d})^2,$$

where Z' runs over all solutions of equation (22). Since $((d_1X_1'^2 + d_2Y_1'^2)/2, X_1'Y_1', 2Z_1')$ is a solution of equation (17), by Lemma 11, we have $2Z_1' = Z_1t$ for some $t \in \mathbf{N}$. If $t > 1$, then $Z_1' \ge Z_1$. By such that same argument as in the proof of Lemma 11, there exists the integers X'', Y'' satisfy

$$d_1X''^2 - d_2Y''^2 = 2^{z_1'-z_1}, \qquad \gcd(X'', Y'') = 1.$$

Recalling that $Z_1' \le Z_1$ and equation (13) has no solution. It is impossible. Therefore $t = 1$ and (25) is proved.

Finally, by such the same argument as in the proof of Lemma 11, we can prove that all solutions of equation (22) are given by (24). The proof is complete.

Lemma 13. *If* $2 \nmid d$, *then there exists at most two distinct pairs* $(d_1, d_2) \in I(d)$ *which make equation* (16) *have solutions* (X, Y).

Proof. Let (d_1, d_2), $(d_1', d_2') \in I(d)$ with $(d_1, d_2) \ne (d_1', d_2')$. We assume that the equations

$$d_1X^2 - d_2Y^2 = 2^{m+2}, \qquad \gcd(X, Y) = 1, \tag{26}$$

and

$$d_1'X'^2 - d_2'Y'^2 = 2^{m+2}, \qquad \gcd(X', Y') = 1, \tag{27}$$

have solutions (X, Y) and (X', Y') respectively. Let $l = \langle X, Y\rangle$ and $l' = \langle X', Y'\rangle$. By Lemma 9, we have $l' \equiv \delta l \pmod{2^{m+2}}$, where $\delta \in \{-1, 1\}$. Further, by Lemma 7, we have

$$d_1X \equiv -lY \pmod{2^{m+2}}, \quad d_1'X' \equiv -l'Y' \equiv -\delta lY' \pmod{2^{m+2}}.$$

Hence

$$\begin{aligned} d_1d_1'XX' &\equiv \delta l^2YY' \equiv \delta dYY' \pmod{2^{m+2}}, \\ d_1\delta lXY' &\equiv d_1'lX'Y \pmod{2^{m+2}}. \end{aligned} \tag{28}$$

Let $d_{11} = \gcd(d_1, d_1')$, $d_{12} = \gcd(d_1, d_2')$, $d_{21} = d_1'/d_{11}$, $d_{22} = d_2'/d_{12}$. Since $d_1d_2 = d_1'd_2' = d$, then $d_1 = d_{11}d_{12}$, $d_2 = d_{21}d_{22}$, $d_1' = d_{11}d_{21}$, $d_2' = d_{12}d_{22}$. Notice that $2 \nmid dll'$. We obtain from (28) that

$$d_{11}XX' - \delta d_{22}YY' \equiv d_{12}XY' - \delta d_{21}X'Y \equiv 0 \pmod{2^{m+2}},$$

whence we get

$$d_{11}XX' - \delta d_{22}YY' = 2^{m+2}X'', \qquad d_{12}XY' - \delta d_{21}X'Y = 2^{m+2}Y'', \tag{29}$$

where $X'', Y'' \in \mathbf{Z}$. By (26) and (27),

$$\begin{aligned} 2^{2m+4} &= (d_1X^2 - d_2Y^2)(d_1'X'^2 - d_2'Y'^2) \\ &= d_1''(d_{11}XX' - \delta d_{22}YY')^2 - d_2''(d_{12}XY' - \delta d_{21}X'Y)^2, \end{aligned} \tag{30}$$

where $d_1'' = d_{12}d_{21}$, $d_2'' = d_{11}d_{22}$ with $d_1''d_2'' = d$. Substituting (29) into (30), we get

$$d_1''X''^2 - d_2''Y''^2 = 1. \tag{31}$$

Since $(d_1, d_2) \ne (d_1', d_2')$ implies $d_{12} > 1$, $d_1'' > 1$, and $(d_1'', d_2'') \in I'(d)$. From (31), such (d_1'', d_2'') is unique by Lemma 6. We note that if (d_1, d_2) is fixed, then the corresponding (d_1'', d_2'') are different for some distinct (d_1', d_2'). This implies the lemma. □

3. Further preliminary lemmas

Throughout this section, we assume that D is a nonsquare. Notice that the least solution of the equation

$$X^2 - DY^2 = 2^{z+2}, \qquad \gcd(X, Y) = 1, \qquad Z > 0, \tag{32}$$

is unique. By Lemmas 12 and 13, the following two lemmas are clear.

Lemma 14. *If there exists two distinct pairs* $(D_1, D_2) \in I'(D)$ *which make the equation*

$$D_1X'^2 - D_2Y'^2 = 2^{Z'+2}, \qquad \gcd(X', Y') = 1, \qquad Z' > 0 \tag{33}$$

have solutions (X', Y', Z'), *then the least solution* (X_1, Y_1, Z_1) *of equation* (32) *satisfies* $2|Z_1$.

Lemma 15. *There exists at most three distinct pairs* $(D_1, D_2) \in I'(D)$ *which make equation* (33) *have solutions* (X', Y', Z'). □

Lemma 16 [1, Lemma 7]. *Suppose there exist integers* a, b, A, B, m *such that*

$$\frac{A + B\sqrt{D}}{2} = \left(\frac{a + b\sqrt{D}}{2}\right)^m, \qquad m > 1, b \neq 0, a \equiv Db \pmod 2.$$

If $D > 1$ *and* $D \equiv 1 \pmod 8$, *then* $|B| > 1$ *except when* $m = 2$ *and* $a, b \in \{-1, 1\}$. □

Lemma 17. *If* (x, n) *is a solution of equation* (1), *then* $(x, 1, n)$ *is a solution of equation* (32). *Let* (X_1, Y_1, Z_1) *be the least solution of equation* (32), *and let* $u_1 + v_1\sqrt{D}$ *be the fundamental solution of the equation*

$$u^2 - Dv^2 = 1. \tag{34}$$

Further let

$$\begin{aligned} \varepsilon &= \frac{X_1 + Y_1\sqrt{D}}{2}, & \overline{\varepsilon} &= \frac{X_1 - Y_1\sqrt{D}}{2}, \\ \rho &= u_1 + v_1\sqrt{D}, & \overline{\rho} &= u_1 - v_1\sqrt{D}. \end{aligned} \tag{35}$$

Then

$$n = Z_1 t, \qquad \frac{x + \delta\sqrt{D}}{2} = \varepsilon^t \overline{\rho}^s, \qquad \delta \in \{-1, 1\}, \tag{36}$$

where $s, t \in \mathbf{Z}$ *satisfy*

$$s \geq 0, \qquad t > 0, \qquad \gcd(s, t) = \begin{cases} 2, & \text{if } 2|s,\ 2|t \text{ and } x = \frac{D+1}{2}, \\ 1, & \text{otherwise.} \end{cases} \tag{37}$$

Proof. By Lemma 11, (36) holds for some $s, t \in \mathbf{Z}$ with $s \geq 0$ and $t > 0$. Moreover, by Lemma 16, s and t satisfy (37). The lemma is proved. □

Lemma 18. *Under the assumption of Lemma* 17, *we have* $\delta \equiv xY_1/X_1 \pmod 4$.

Proof. Let

$$\frac{X + Y\sqrt{D}}{2} = \varepsilon^t, \qquad u - v\sqrt{D} = \overline{\rho}^s. \tag{38}$$

By Lemma 1, we have $X, Y \in \mathbf{Z}$ satisfy

$$\begin{aligned} X = \varepsilon^t + \overline{\varepsilon}^t &= \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} (\varepsilon + \overline{\varepsilon})^{t-2i} (\varepsilon\overline{\varepsilon})^i = \sum_{i=0}^{[t/2]} (-1)^i \begin{bmatrix} t \\ i \end{bmatrix} X_1^{t-2i} 2^{Z_1 i} \\ &\equiv \begin{cases} X_1^t - 2tX_1^{t-2} \pmod 4, & \text{if } Z_1 = 1, \\ X_1^t \pmod 4, & \text{if } Z_1 > 1, \end{cases} \end{aligned} \tag{39}$$

$$(40)\qquad Y=\frac{\varepsilon^t-\bar{\varepsilon}^t}{\sqrt{D}}\equiv\begin{cases} Y_1^t+2tY_1^{t-2}\pmod 4, & \text{if } Z_1=1,\ 2\nmid t,\\ (Y_1^{t'}+2t'Y_1^{t'-2})(X_1^{t'}-2t'X_1^{t'-2})\pmod 4, & \\ \qquad\qquad \text{if } Z_1=1,\ t=2^\alpha t',\ \alpha>0,\ 2\nmid t', & \\ Y_1^t\pmod 4, & \text{if } Z_1>1,\ 2\nmid t,\\ Y_1^{t'}X_1^{t-t'}\pmod 4 & \text{if } Z_1>1,\ t=2^\alpha t',\ \alpha>0,\ 2\nmid t', \end{cases}$$

since $D\equiv 1\pmod 8$. Notice that $4\mid v$ when $D\equiv 1\pmod 8$. Then from

$$(41)\qquad \frac{x+\delta\sqrt{D}}{2}=\left(\frac{X+Y\sqrt{D}}{2}\right)(u-v\sqrt{D}),$$

we get $x=Xu-DYv\equiv Xu\pmod 4$ and $\delta=Yu-Xv\equiv Yu\pmod 4$, and so

$$(42)\qquad \delta\equiv\frac{xY}{X}\pmod 4.$$

Since $X_1^2\equiv DY_1^2\pmod 8$, substituting (39) and (40) into (42), the lemma is proved. $\square$

Lemma 19. *If (x, n) is a solution of equation (1) with $2\mid n$, then $2^n<D^2/16$.*

Proof. Under the assumption, we have $x+2^{n/2+1}=D_1$ and $x-2^{n/2+1}=D_2$, where $(D_1, D_2)\in I(D)$. It follows that $2^{n/2+2}=D_1-D_2\le D-1<D$. Thus the lemma. $\square$

Lemma 20. *If (x, n) is a solution of equation (1) with $2\nmid n$, then $2\nmid Z_1t$ and $(x, 2^{Z_1((t-1)/2)})$ is a solution of the equation*

$$(43)\qquad x'^2-2^{Z_1+2}y'^2=D,\quad \gcd(x', y')=1,$$

satisfying

$$\langle x', 2^{Z_1((t-1)/2)}\rangle\equiv\begin{cases} -X_1\pmod D, & \text{if } 2\mid s,\\ -X_1u_1\pmod D, & \text{if } 2\nmid s.\end{cases}$$

Proof. By Lemma 7, we have

$$(44)\qquad \langle x, 2^{z_1((t-1)/2)}\rangle\equiv-\frac{x}{2^{z_1((t-1)/2)}}\pmod D.$$

From (38) and (41), we get

$$(45)\qquad \begin{aligned} x\equiv Xu\equiv\frac{X_1^tu_1^s}{2^{t-1}}&\equiv 2^{z_1((t-1)/2)}X_1u_1^s\\ &\equiv\begin{cases} 2^{z_1((t-1)/2)}X_1\pmod D, & \text{if } 2\mid s,\\ 2^{z_1((t-1)/2)}X_1u_1\pmod D, & \text{if } 2\nmid s,\end{cases}\end{aligned}$$

since $2\nmid Z_1t$, $X_1^2\equiv 2^{z_1+2}\pmod D$ and $u_1^2\equiv 1\pmod D$. Substituting (45) into (44), we obtain the lemma. $\square$

Lemma 21. *Let (X_1, Y_1, Z_1) be the least solution of equation (32). If $2^{rz_1+2}<\sqrt{D}$ for some $r\in\mathbf{N}$, then the fundamental solution $\rho=u_1+v_1\sqrt{D}$ of equation (34) satisfies $\rho>D^{r/2}/2^{2r-2}$.*

Proof. By Lemma 11, there exists $X_i, Y_i\in\mathbf{Z}$ $(i=1,\dots,\gamma)$ such that

$$X_i^2-DY_i^2=2^{z_1i+2},\qquad \gcd(X_i, Y_i)=1,\qquad i=1,\dots,r.$$

Since $2^{rz_1+2} < \sqrt{D}$, by (v) of Lemma 5, $\sqrt{D}$ has $2r$ convergents p_{s_i}/q_{s_i} and p_{t_i}/q_{t_i} $(i = 1, \dots, \gamma)$ such that

$$k_{s_i} = k_{t_i} = 2^{z_1 i+2}, \qquad 2 \nmid s_i t_i, \, 0 < s_i, \, t_i < t, \, i = 1, \dots, \gamma,$$

where t was defined in (iii) of Lemma 5. Therefore, by (i) of Lemma 5, we have

$$\begin{aligned} a_{s_i+1} &= \left[\frac{\Delta_{s_i} + \sqrt{D}}{k_{s_i}}\right] > \frac{\sqrt{D}}{2^{z_1 i+2}}, \\ a_{t_i+1} &= \left[\frac{\Delta_{t_i} + \sqrt{D}}{k_{t_i}}\right] > \frac{\sqrt{D}}{2^{z_1 i+2}}, \qquad i = 1, \dots, r. \end{aligned} \tag{46}$$

Notice where $p_0 = a_0$, $p_1 = a_0 a_1 + 1$, and $p_{j+2} = a_{j+2} p_{j+1} + p_j$ for $j \geq 0$. By (iii) of Lemma 5, we deduce from (46) that

$$\begin{aligned} \rho > u_1 = p_t &> \prod_{j=0}^{t} a_j \geq a_0 \prod_{i=1}^{\gamma} a_{s_i} a_{t_i} \\ &> a_0 \left(\prod_{i=1}^{\gamma} \frac{\sqrt{D}}{2^{z_1 i+2}}\right)^2 = \frac{a_0 D^r}{2^{r(r+1)z_1+4r}} > \frac{D^{r/2}}{2^{2r-2}}, \end{aligned}$$

since $a_0 = [\sqrt{D}]$. The lemma is proved. □

Lemma 22 [1, Lemma 6 and the proof of Theorem 3]. *Let* (x, n), (x', n'), (x'', n'') *be three solutions of equation* (1) *with* $n'' > n' > n$. *We have:*

(i) *If* $x' - x = 2$, *then either* D *is of type* I *or* D *is of type* III *and* $(x, x') = (2^{m_2} - 2^{m_1} - 1, 2^{m_2} - 2^{m_1} + 1)$.

(ii) *If* $x' - x = 4$, *then* D *is of type* I.

(iii) *If* D *is of type* II *and* $(x, x', x'') = ((2^{2m+1} - 17)/3, (2^{2m+1} + 1)/3, (17 \cdot 2^{2m+1} - 1)/3)$, *then* $n'' = 2n' + 3$.

(iv) *With the exception of above cases,* $x' - x \geq 6$ *and* $n'' \geq 2n' + 53$. □

Lemma 23 [1, Corollaries 1 and 2]. *If* (χ, n) *is a solution of equation* (1), *then* $n < 433 + (10 \log D)/\log 2$. *Moreover, if* $D < 2^{96}$, *then* $n < 16 + (2 \log D)/\log 2$. □

4. Proof of theorem

By Theorems 3 and 4 of [1], it suffices to prove that $N(D) = 3$ while $D \geq 10^{12}$ and D is of types II or III. Moreover, if D is a square, then $N(D) \leq 1$. We may assume that D is not a square.

Assertion 1. *If* D *is of type* II, *then* $N(D) = 3$.

Proof. In this case, equation (1) has three solutions

$$\begin{aligned} (x_1, n_1) &= \left(\frac{2^{2m+1} - 17}{3}, 3\right), \qquad (x_2, n_2) = \left(\frac{2^{2m+1}}{3}, 2m + 1\right), \\ (x_3, n_3) &= \left(\frac{17 \cdot 2^{2m+1} - 1}{3}, 4m + 5\right). \end{aligned} \tag{47}$$

By the proof of Theorem 3 of [1], if $N(D) > 3$, then equation (1) has another solution (x_4, n_4) with $n_4 > n_3$. By Lemmas 19 and 22, we see that $2 \nmid n_4$. Let (X_1, Y_1, Z_1) be the least solution of (32), and let $\varepsilon, \overline{\varepsilon}, \rho, \overline{\rho}$ be defined as in (35). Then, by Lemma 17, we have

$$(48) \qquad n_i = Z_i t_i, \quad \frac{\chi_i + \delta_i\sqrt{D}}{2} = \varepsilon^{t_i}\overline{\rho}^{s_i}, \qquad \delta_i \in \{-1, 1\}, i = 1, \dots, 4,$$

where $s_i, t_i \in \mathbf{Z}$ $(i = 1, \dots, 4)$ satisfy

$$(49) \qquad s_i \geq 0, \qquad t_i > 0, \qquad \gcd(s_i, t_i) = 1, \qquad i = 1, \dots, 4.$$

We see from (47) and (48) that equation (43) has three solutions $(x_j, 2^{z_1((t_j-1)/2)})$ $(j = 2, 3, 4)$. Let $l_j = \langle x_j, 2^{z_1((t_j-1)/2)}\rangle$ $(j = 2, 3, 4)$. By Lemma 7, we get from (47) and (48) that

$$\begin{aligned} l_2 - l_3 &\equiv -\frac{2^{2m+1}+1}{3 \cdot 2^{z_1((t_2-1)/2)}} + \frac{17 \cdot 2^{2m+1} - 1}{3 \cdot 2^{z_1((t_3-1)/2)}} \\ &\equiv -\frac{2^{(z_1-1)/2}}{3 \cdot 2^{2m+2}}(2^{3m+3} - 17 \cdot 2^{2m+1} + 2^{m+2} + 1) \not\equiv 0 \pmod{D}. \end{aligned}$$

It follows that $l_2 \neq l_3$. Further, by Lemma 20, we have either $l_4 = l_2$ or $l_4 = l_3$. Furthermore, by Lemma 8, we get

$$\begin{aligned} &x_4 + 2^{z_1((t_4-1)/2)}\sqrt{2^{z_1+2}} \\ &\quad = \begin{cases} (x_2 + 2^{z_1((t_2-1)/2)}\sqrt{2^{z_1+2}}(U' + V'\sqrt{2^{z_1+2}}), & \text{if } l_4 = l_2, \\ (x_3 + 2^{z_1((t_3-1)/2)}\sqrt{2^{z_1+2}})(U' + V'\sqrt{2^{z_1+2}}), & \text{if } l_4 = l_3, \end{cases} \end{aligned}$$

and hence

$$(50) \qquad 2^{z_1((t_4-1)/2)} = \begin{cases} x_2 V' + 2^{z_1((t_2-1)/2)}U', & \text{if } l_4 = l_2, \\ x_3 V' + 2^{z_1((t_3-1)/2)}U', & \text{if } l_4 = l_3, \end{cases}$$

where (U', V') is a positive solution of the equation

$$(51) \qquad U'^2 - 2^{z_1+2}V'^2 = 1.$$

Since $t_3 > t_2$, we obtain

$$(52) \qquad 2^{z_1((t_2-1)/2)} \mid V'$$

by (50). On applying Lemma 3 with (52), we have

$$(53) \qquad U' + V'\sqrt{2^{z_1+2}} = (3 + 2\sqrt{2})^{2^{m\gamma}}, \qquad \gamma \in \mathbf{N},$$

since $Z_1 t_2 = 2m + 1$. From (53), we deduce $2U' > 2^{5\cdot 2^{m-1}}$ and

$$(54) \qquad n_4 > 2m + 1 + 5 \cdot 2^m$$

by (47), (48), and (50). On the other hand, by Lemma 23, we have

$$(55) \qquad n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 40m$$

since $D < 2^{4m}$. The combination of (54) and (55) yields $m \leq 7$ and $D < 2^{4m} \leq 2^{28} < 10^{12}$. Thus the assertion is proved. $\square$

Assertion 2. *If D is of type* III, *then* $N(D) = 3$.

Proof. In this case, equation (1) has three solutions

$$(56) \qquad \begin{aligned} (x_1, n_1) &= (2^{m_2} - 2^{m_1} - 1, m_1), \\ (x_2, n_2) &= (2^{m_2} - 2^{m_1} + 1, m_2), \\ (x_3, n_3) &= (2^{m_2} + 2^{m_1} - 1, m_2 + m_1). \end{aligned}$$

If $N(D) > 3$, then equation (1) has another solution (χ_4, n_4) with $n_4 > n_3$. Moreover, then (48) and (49) still hold by Lemma 17.

When $2|m_1$ and $2|m_2$, we get from (56) that

$$D_{11} - D_{12} = 2^{m_1/2+2}, \qquad D_{21} - D_{22} = 2^{m_2/2+2},$$

where

$$\begin{aligned} D_{11} &= 2^{m_2} - 2^{m_1} + 2^{m_1/2+1} - 1, & D_{12} &= 2^{m_2} - 2^{m_1} - 2^{m_1/2+1} - 1, \\ D_{21} &= 2^{m_2} + 2^{m_2/2+1} - 2^{m_1} + 1, & D_{22} &= 2^{m_2} - 2^{m_2/2+1} - 2^{m_1} + 1. \end{aligned}$$

Since $(D_{11}, D_{12}), (D_{21}, D_{22}) \in I'(D)$ and $(D_{11}, D_{12}) \neq (D_{21}, D_{22})$, by Lemma 14, the least solution of equation (32) satisfies $2|Z_1$. Therefore, $2|n_4$ by (48). Then we have

$$D_{31} - D_{32} = 2^{(m_2+m_1)/2+2}, \qquad D_{41} - D_{42} = 2^{n_4/2+2},$$

where

$$\begin{aligned} D_{31} &= 2^{m_2} + 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1, & D_{32} &= 2^{m_2} - 2^{(m_2+m_1)/2+1} + 2^{m_1} - 1, \\ D_{41} &= x_4 + 2^{n_4/2+1}, & D_{42} &= x_4 - 2^{n_4/2+1}. \end{aligned}$$

Since (D_{31}, D_{32}), $(D_{41}, D_{42}) \in I'(D)$, and (D_{i1}, D_{i2}) $(i = 1, \ldots, 4)$ are different, this implies that there exist four distinct pairs $(D_1, D_2) \in I'(D)$ which make equation (33) have solutions. By Lemma 15, it is impossible.

When $2 \mid m_1$ and $2 \nmid m_2$, we have $2 \nmid Z_1$ by (48). If $2 \mid n_4$, since $2 \mid m_1$, we see from Lemma 14 that $2 \mid Z_1$, a contradiction. Therefore $2 \nmid n_4$ and equation (43) has three solutions $(x_j, 2^{z_1((t_j-1)/2)})$ $(j = 2, 3, 4)$. Let $l_j = \langle x_j, 2^{z_1((t_j-1)/2)} \rangle$ $(j = 2, 3, 4)$. From (56), we get

$$\begin{aligned} l_2 - l_3 &\equiv -\frac{2^{m_2} - 2^{m_1} + 1}{2^{z_1((t_2-1)/2)}} + \frac{2^{m_2} + 2^{m-1} - 1}{2^{z_1((t_3-1)/2)}} \\ &\equiv \frac{2^{(z_1-1)/2}}{2^{(m_2+m_1-1)/2}}(-2^{m_1/2}(2^{m_2} - 2^{m_1} + 1) + (2^{m_2} + 2^{m_1} - 1)) \not\equiv 0 \pmod{D}. \end{aligned}$$

It follows that $l_2 \neq l_3$ and either $l_4 = l_2$ or $l_4 = l_3$ by Lemma 20. By such the same argument as in the proof of Assertion 1, then (50) and (52) still hold. Hence

$$U' + V'\sqrt{2^{z_1+2}} = (3 + 2\sqrt{2})^{2^{(m_2-1)/2}\gamma}, \qquad \gamma \in \mathbf{N},$$

whence we get $2U' > 2^{5\cdot 2^{(m_2-3)/2}}$. On applying this with (50), we obtain

$$(57) \qquad n_4 > m_2 + 5 \cdot 2^{(m_2-3)/2}.$$

On the other hand, since $\sqrt{D} < 2^{m_2}$, we have

$$(58) \qquad n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 20m_2$$

by Lemma 23. The combination of (57) and (58) yields $m_2 \leq 17$ and $D < 2^{34} < 10^{12}$, which is in contradiction with the assumption.

Let $2 \nmid m_1 m_2$ and $3.6m_1 \geq m_2$. Since $2 \mid m_2 + m_1$, we have $2 \nmid n_4$, and equation (43) has three solutions $(x_j, 2^{z_1((t_j-1)/2)})$ $(j = 1, 2, \dots, 4)$. Let $l_j = \langle x_j, 2^{z_1((t_j-1)/2)} \rangle$ $(j = 1, 2, 4)$. By Lemma 7, we obtain $l_1 \neq l_2$. Furthermore, by Lemma 20, we have either $l_4 = l_1$ or $l_4 = l_2$. By such the same argument as in the case that $2 \mid m_1$ and $2 \nmid m_2$, we can prove $l_4 \neq l_2$. If $l_4 = l_1$, we have

$$x_4 + 2^{z_1((t_4-1)/2)}\sqrt{2^{z_1+2}} = (2^{m_2} - 2^{m_1} - 1 + 2^{z_1((t_1-1)/2)}\sqrt{2^{z_1+2}})(U' + V'\sqrt{2^{z_1+2}}),$$

whence we get

$$2^{z_1((t_4-1)/2)} = (2^{m_2} - 2^{m_1} - 1)V' + 2^{z_1((t_1-1)/2)}U',$$

where $U', V' \in \mathbf{N}$ satisfy (51). Hence $2^{z_1((t_1-1)/2)} | V'$ and

$$2^{z_1((t_4-t_1)/2)} = (2^{m_2} - 2^{m_1} - 1)\frac{V'}{2^{z_1((t_1-1)/2)}} + U'. \tag{59}$$

Further, by Lemma 3, we have

$$U' + V'\sqrt{2^{z_1+2}} = (3 + 2\sqrt{2})^{2^{(m_1-1)/2}\gamma}, \qquad \gamma \in \mathbf{N}, \tag{60}$$

since $m_1 = Z_1 t_1$ and $2 \nmid Z_1$. Furthermore, we see from (60) that $U' \equiv 1 \pmod 8$ and

$$\frac{V'}{2^{z_1((t_1-1)/2)}} \equiv 3^{2^{(m_1-1)/2}r-1}\gamma \equiv 3r \pmod 8$$

since $m_1 \geq 3$. Hence, we obtain $\gamma \equiv 3 \pmod 8$ by (59). It implies that $\gamma \geq 3$ and

$$2U' > 2^{15 \cdot 2^{(m_1-3)/2}}$$

by (60). On applying this with (59), we get

$$n_4 > m_1 + 15 \cdot 2^{(m_1-1)/2} - 2. \tag{61}$$

On the other hand, by Lemma 23,

$$n_4 < 433 + 10\frac{\log D}{\log 2} < 433 + 20m_2 \leq 433 + 72m_1. \tag{62}$$

The combination of (61) and (62) yields $m_1 \leq 13$ and $D < 2^{2m_2} \leq 2^{7.2m_1} < 2^{96}$. On applying Lemma 23 again, we have

$$n_4 < 16 + 2\frac{\log D}{\log 2} < 16 + 4m_2 \leq 16 + 14.4m_1.$$

On combining this with (61), we get $m_1 \leq 5$ and $D < 2^{36} < 10^{12}$. Thus $N(D) = 3$.

Using the same method, we can prove the assertion for the case that $2 \nmid m_1$, $2 \mid m_2$, and $m_2 \leq 3.6m_1$.

Let $2 \nmid m_1$ and $m_2 > 3.6m_1$. We obtain from (48) that

$$\left(\frac{x_2 + \delta_2\sqrt{D}}{2}\right)^{t_3} \rho^{s_2 t_3} = \left(\frac{x_3 + \delta_3\sqrt{D}}{2}\right)^{t_2} \rho^{s_3 t_2}. \tag{63}$$

Since $x_2 \equiv 1 \pmod 4$ and $x_3 \equiv -1 \pmod 4$, we have

$$\delta_2 = -\delta_3 \tag{64}$$

by Lemma 18. Since $2^{m_2} - 2^{m_1} - 2 < \sqrt{D} < 2^{m_2} - 2^{m_1} - 1$, we have

$$t_3 \log \frac{x_2 + \sqrt{D}}{2} + t_2 \log \frac{x_3 + \sqrt{D}}{2} > t_2 t_3 \log 2^{z_1}$$

by (48) and (56). Hence, from (63) and (64),

(65)

$$\begin{aligned} |s_2 t_3 - s_3 t_2| \log \rho &= \left| t_3 \log \frac{x_2 + \delta_2 \sqrt{D}}{2} - t_2 \log \frac{x_3 + \delta_3 \sqrt{D}}{2} \right| \\ &= t_3 \log \frac{x_2 + \sqrt{D}}{2} + t_2 \log \frac{x_3 + \sqrt{D}}{2} - t_2 t_3 \log 2^{z_1} \\ &< t_3 \log \tfrac{1}{2}((2^{m_2} - 2^{m_1} + 1) + (2^{m_2} - 2^{m_1} - 1)) \\ &\quad + t_2 \log \tfrac{1}{2}((2^{m_2} + 2^{m_1} - 1) + (2^{m_2} - 2^{m_1} - 1)) - t_3 \log 2^{m_2} \\ &< t_2 \log 2^{m_2}. \end{aligned}$$

Notice that only one of n_2 and n_3 is even. We see from (49) that $2 \nmid s_2 t_3 - s_3 t_2$. If $|s_2 t_3 - s_3 t_2| > 1$, then $|s_2 t_3 - s_3 t_2| \geq 3$ and

$$3 \log \rho < t_2 \log 2^{m_2} \tag{66}$$

by (65). Recalling that $m_2 = Z_1 t_2$ and $2 \nmid Z_1$. Since $2^{m_2 - 1} < \sqrt{D} < 2^{m_2}$, we get

$$\sqrt{D} > \begin{cases} 2^{(t_2 - 3) z_1 + 2}, & \text{if } Z_1 = 1, \\ 2^{(t_2 - 1) z_1 + 2}, & \text{if } Z_1 > 1. \end{cases}$$

By Lemma 21, we have

$$\log \rho > \begin{cases} (t_2 - 3) \log \sqrt{D} - (t_2 - 4) \log 4, & \text{if } Z_1 = 1, \\ (t_2 - 1) \log \sqrt{D} - (t_2 - 2) \log 4, & \text{if } Z_1 > 1. \end{cases} \tag{67}$$

Recalling that $D \geq 10^{12}$. The combination of (66) and (67) yields

$$t_2 \leq \begin{cases} 4, & \text{if } Z_1 = 1, \\ 2, & \text{if } Z_1 > 1, \end{cases}$$

a contradiction. Thus

$$s_2 t_3 - s_3 t_2 = \pm 1. \tag{68}$$

Let $\alpha = (\log(\varepsilon / \bar{\varepsilon})) / \log \rho^2$, and let

$$\Lambda(x, n) = \log \frac{x + \sqrt{D}}{x - \sqrt{D}},$$

for any solution (x, n) of equation (1). Then we have

$$\alpha - \frac{s_i}{t_i} = \frac{\delta_i \Lambda(x_i, n_i)}{t_i \log \rho^2}, \qquad i = 1, \dots, 4, \tag{69}$$

by (48). We see from (64) that α lies in the interval $(s_2/t_2, s_3/t_3)$. Moreover, since $t_4 > t_j$ and $\Lambda(x_4, n_4) < \Lambda(x_j, n_j)$ for $j = 2, 3$, we see from (69) that s_4/t_4 lies in the interval $(s_2/t_2, s_3/t_3)$ too. By Lemma 2, we get from (68) that

$$t_4 = c t_2 + c' t_3, \qquad s_4 = c s_2 + c' s_3, \qquad c, c' \in \mathbf{N}. \tag{70}$$

From (48) and (70), we have

$$\frac{x_4+\delta_4\sqrt{D}}{2}=\varepsilon^{t_4}\overline{\rho}^{s_4}=\left(\frac{x_2+\delta_2\sqrt{D}}{2}\right)^c\left(\frac{x_3+\delta_3\sqrt{D}}{2}\right)^{c'}. \tag{71}$$

Let

$$\frac{X_2+Y_2\sqrt{D}}{2}=\left(\frac{x_2+\delta_2\sqrt{D}}{2}\right)^c,\qquad \frac{X_3+Y_3\sqrt{D}}{2}=\left(\frac{x_3+\delta_3\sqrt{D}}{2}\right)^{c'}. \tag{72}$$

Then X_2, Y_2, X_3, Y_3 are integers. Let $\varepsilon_2=(x_2+\delta_2\sqrt{D})/2$, and $\overline{\varepsilon}_2=(x_2-\delta_2\sqrt{D})/2$. Since $\varepsilon_2+\overline{\varepsilon}_2=x_2\equiv 1-2^{m_1} \pmod{2^{m_2}}$ and $\varepsilon_2\overline{\varepsilon}_2=2^{m_2}\equiv 0 \pmod{2^{m_2}}$, by Lemma 1, we have

$$\varepsilon_2^m+\overline{\varepsilon}_2^m=\sum_{i=0}^{[m/2]}(-1)^i\left[\begin{matrix}m\\ i\end{matrix}\right](\varepsilon_2+\overline{\varepsilon}_2)^{m-2i}(\varepsilon_2\overline{\varepsilon}_2)^i\equiv(1-2^{m_1})^m \pmod{2^{m_2}}$$

for any $m\in\mathbf{N}$. It follows that $X_2\equiv(1-2^{m_1})^c \pmod{2^{m_2}}$. Simultaneously, we have

$$\begin{aligned}Y_2&=\frac{\varepsilon_2^c-\varepsilon_2^c}{\sqrt{D}}=\delta_2\frac{\varepsilon_2^c-\overline{\varepsilon}_2^c}{\varepsilon_2-\overline{\varepsilon}_2}\\ &=\delta_2\left((\varepsilon_2^{c-1}+\overline{\varepsilon}_2^{c-1})+\varepsilon_2\overline{\varepsilon}_2\left(\frac{\varepsilon_2^{c-2}-\overline{\varepsilon}_2^{c-2}}{\varepsilon_2-\overline{\varepsilon}_2}\right)\right)\\ &\equiv\delta_2(\varepsilon_2^{c-1}+\overline{\varepsilon}_2^{c-1})\equiv\delta_2(1-2^{m_1})^{c-1} \pmod{2^{m_2}}.\end{aligned}$$

By the same argument, we can get $X_3\equiv(-1+2^{m_1})^{c'} \pmod{2^{m_2}}$ and $Y_3\equiv\delta_3(-1+2^{m_1})^{c'-1} \pmod{2^{m_2}}$, since $x_3=2^{m_2}+2^{m_1}-1$. From (64), (71) and (72),

$$\begin{aligned}2\delta_4&=X_2Y_3+X_3Y_2\\ &\equiv\delta_3(1-2^{m_1})^c(-1+2^{m_1})^{c'-1}+\delta_2(1-2^{m_1})^{c-1}(-1+2^{m_1})^{c'}\\ &\equiv(-1)^{c'}2\delta_2(1-2^{m_1})^{c+c'-1} \pmod{2^{m_2}}.\end{aligned}$$

It follows that

$$\pm1\equiv(1-2^{m_1})^{c+c'-1} \pmod{2^{m_2-1}},$$

whence we deduce that $c+c'-1\equiv 0 \pmod{2^{m_2-m_1-1}}$. Since $m_1\geq 3$ and $m_2>3.6m_1$, we have $c+c'-1>2^{2.6m_1-1}>2^{6.8}>96$. Hence, from (48), (56) and (70), we get

$$n_4=cm_2+c'(m_2+m_1)>(c+c')m_2>96m_2>48\frac{\log D}{\log 2}, \tag{73}$$

since $\sqrt{D}<2^{m_2}$. On applying Lemma 23 with (73), we obtain $D<2^{20}<10^{12}$. Thus $N(D)=3$. All cases are considered and the assertion is proved.

The combination of Assertions 1 and 2 yields the theorem.

Acknowledgment

The author would like to thank Professor A. Schinzel and the referee for their valuable suggestions.

REFERENCES

1. F. Beukers, *On the generalized Ramanujan-Nagell equation*. I, Acta Arith. **38** (1980/1981), 389–410.

2. L.-K. Hua, *Introduction to number theory*, Springer-Verlag, Berlin, 1982.

3. R. Lidl and H. Niederreiter, *Finite fields*, Addison-Wesley, Reading, Mass., 1983.

4. T. Nagell, *Contributions to the theory of a category of diophantine equations of the second degree with two unknowns*, Nova Acta Soc. Sci. Upsala (4) **16** (1955), 38 pp.

RESEARCH DEPARTMENT, CHANGSHA RAILWAY INSTITUTE, CHANGSHA, HUNAN, PEOPLES REPUBLIC OF CHINA